

Best Available Copy

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-265723

(43)Date of publication of application : 11.10.1996

(51)Int.Cl.

H04N 7/167

H04L 9/06

H04L 9/14

H04N 7/24

(21)Application number : 07-067743

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 27.03.1995

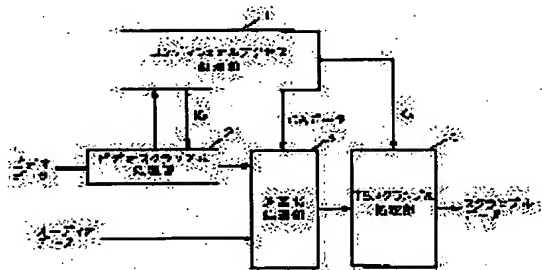
(72)Inventor : KATSUTA NOBORU  
MURAKAMI HIRONORI  
IBARAKI SUSUMU

## (54) SCRAMBLE CONTROL METHOD, SCRAMBLE DEVICE AND DE-SCRAMBLE DEVICE

(57)Abstract:

**PURPOSE:** To unify a key of scramble(SC) in video and system levels and to shorten reproducing time by using a head position of a video sequence as the updating timing of the SC key in the case of an SC control of data during an MPEG transport stream.

**CONSTITUTION:** A conditional access processing part 1 sends a scramble key Ks to a video SC processing part 2 and a TSSC processing part 4 and sends CA data including the Ks to a multiplex processing part 3. The CA data include the key Ks and signals exhibiting for which data a scramble process is to be performed. Video data are SC-processed by the SC key Ks from the processing part 1 in the processing part 2 and sent to the processing part 3. Here, the processing part 2 detects the head of the video sequence and sends detection signals to the processing part 1. In the processing part 1, the SC key which is valid in TS scramble at present is sent. In the processing part 2, it is turned to a valid key immediately after receiving it and the SC processing is performed. The processing part 3 attaches 11 or 10 to the SC control code of the packet of the CA data, turns them to the packets to multiplex, and also generates CA packet data from the CA data, turns them to the packets to multiplex and outputs XSC data through the processing part 4.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the

Best Available Copy

examiner's decision of rejection or application  
converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of  
rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

特開平8-265723

(43) 公開日 平成8年(1996)10月11日

(51) Int.Cl. <sup>4</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 N	7/167		H 0 4 N 7/167	
H 0 4 L	9/06		H 0 4 L 9/02	Z
	9/14		H 0 4 N 7/13	Z
H 0 4 N	7/24			

審査請求 未請求 請求項の数13 O L (全 13 頁)

(21) 出願番号 特願平7-67743

(22) 出願日 平成7年(1995)3月27日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 勝田 昇

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72) 発明者 村上 弘規

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(72) 発明者 茂木 晋

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

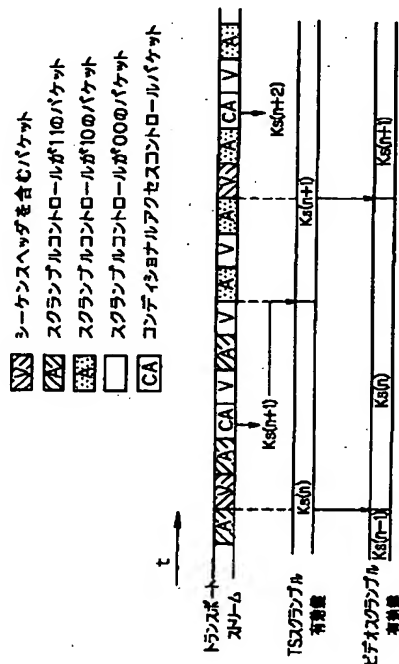
(74) 代理人 弁理士 滝本 智之 (外1名)

(54) 【発明の名称】 スランブル制御方法およびスランブル装置およびデスクランブル装置

(57) 【要約】

【目的】 本発明は、データの伝送あるいは保管に際し、再生者を限定するスランブル制御に関するものでビデオレベルでのスランブルとシステムレベルでのスランブルの鍵の一元化、再生時間の短縮等を目的とする。

【構成】 スランブル鍵は、CAパケット中で送られる。また、スランブル処理は、オーディオデータにはパケット単位でスランブル処理を行い、ビデオデータにはビデオレベルのスランブル処理を行う。パケット単位のスランブルの制御は、スランブルの対象となるパケットのスランブルコントロールコードパターンの“11”と“10”の変わりめで更新する。ビデオレベルスランブルの鍵更新タイミングは、ビデオシーケンスの先頭であり、そのときTSスランブルの有効鍵をビデオスランブルの有効鍵とする。



Best Available Copy

#### 【特許請求の範囲】

【請求項1】MPEG標準に準拠したデジタル信号をトランスポートパケット単位で送信し、各データにスクランブルを施してなるスクランブル制御方法において、MPEG標準に準拠したビデオデータ中のビデオシーケンスの先頭をスクランブル鍵の更新タイミングとして用いることを特徴とするスクランブル制御方法。

【請求項2】送信データがビデオ以外のデータを少なくとも1つ含み、ビデオ以外のデータの少なくとも1つがトランスポートパケット単位でスクランブルの処理が施され、そのスクランブル鍵の更新タイミングがトランスポートパケットヘッダ中のスクランブルコントロール信号により制御されており、ビデオデータのビデオシーケンスのヘッダにより規定されたビデオデータに対するスクランブル鍵更新タイミングにおいてビデオデータに対するスクランブル鍵を、前記トランスポート単位で施されているデータに対して使用中のスクランブル鍵に更新することを特徴とする請求項1記載のスクランブル制御方法。

【請求項3】ビデオデータをトランスポートパケット単位でスクランブル処理するスクランブル制御方法において、ビデオデータのビデオシーケンスの先頭を含むパケットを鍵更新タイミングとすることを特徴とするスクランブル制御方法。

【請求項4】少なくとも1ピクチャーより長い更新周期で伝送されるスクランブル鍵とピクチャテンポラルリファレンスより決定されるパラメータをスクランブルを行うパラメータとしてピクチャの先頭毎に適用することを特徴とするスクランブル制御方法。

【請求項5】少なくとも1スライスより長い更新周期で伝送されるスクランブル鍵とピクチャテンポラルリファレンスおよびスライスパーティカルポジションより決定されるパラメータをスクランブルを行うパラメータとしてスライスの先頭において前記パラメータを更新することを特徴とするスクランブル制御方法。

【請求項6】前記請求項5のスクランブル制御方法において、さらに、ピクチャの先頭でスクランブル鍵とピクチャテンポラルリファレンスより決定されるパラメータによりスクランブルを行うパラメータを更新することを特徴とするスクランブル制御方法。

【請求項7】ビデオデータにスクランブル処理するビデオスクランブル手段とトランスポートパケット単位でスクランブル処理を施すトランスポートスクランブル手段と前記ビデオスクランブル手段とトランスポートスクランブル手段にスクランブル鍵を更新させるスクランブル鍵更新手段からなり、スクランブル鍵更新手段は、ビデオスクランブル処理手段にビデオデータのビデオシーケンスの先頭毎にスクランブル鍵を更新させ、前記更新されるスクランブル鍵は、前記ビデオシーケンスにおいてスクランブルされたビデオデータ中のビデオシーケンス

コードを含むパケット以前に伝送されたパケットで最も最近スクランブルされたパケットのスクランブル処理に用いられたスクランブル鍵と等しい鍵であることを特徴とするスクランブル装置。

【請求項8】トランスポートパケット単位でデスクランブル処理するトランスポートデスクランブル手段とスクランブルを施されてなるビデオデータをデスクランブル処理するビデオデスクランブル手段と前記二つのデスクランブル手段のスクランブル鍵を更新する鍵更新手段を具備し、ビデオデスクランブル手段がビデオシーケンスの先頭で鍵を更新し、鍵更新手段は、ビデオデスクランブル手段が鍵を更新する際、その更新鍵を前記ビデオシーケンスの先頭が含まれていたトランスポートパケットの直前でスクランブルされているパケットをデスクランブル処理したスクランブル鍵と同じ鍵とすることを特徴とするデスクランブル装置。

【請求項9】MPEG標準に準拠したビデオデータをスクランブル処理するビデオデータ攪拌処理手段とスクランブルパラメータ生成手段とピクチャテンポラルリファレンス検出手段を具備し、ピクチャの先頭において、スクランブル鍵およびテンポラルリファレンスにより規定されるスクランブルパラメータを生成し、ビデオデータ攪拌処理部は、前記スクランブルパラメータを用いてスクランブル処理することを特徴とするスクランブル装置。

【請求項10】スクランブルが施されてなるMPEG標準に準拠したビデオデータをデスクランブル処理するビデオデータデスクランブル処理手段とスクランブルパラメータ生成手段とピクチャテンポラルリファレンス検出手段を具備し、ピクチャの先頭において、スクランブル鍵およびテンポラルリファレンスにより規定されるスクランブルパラメータを生成し、ビデオデータデスクランブル処理部は、前記スクランブルパラメータを用いてデスクランブル処理することを特徴とするデスクランブル装置。

【請求項11】MPEG標準に準拠したビデオデータをスクランブル処理するビデオデータ攪拌処理手段とスクランブルパラメータ生成手段とピクチャテンポラルリファレンス検出手段とスライスパーティカルポジション検出手段を具備し、スライスの先頭において、スクランブル鍵およびスライスが属しているピクチャのテンポラルリファレンスおよびスライスパーティカルポジションにより規定されるスクランブルパラメータを生成し、ビデオデータ攪拌処理部は、前記スクランブルパラメータを用いてスクランブル処理することを特徴とするスクランブル装置。

【請求項12】スクランブルが施されてなるMPEG標準に準拠したビデオデータをデスクランブル処理するビデオデータデスクランブル処理手段とスクランブルパラメータ生成手段とピクチャテンポラルリファレンス検

出手段とスライスパーティカルポジション検出手段を具備し、スライスの先頭において、スクランブル鍵およびスライスが属しているピクチャのテンポラルリファレンスおよびスライスパーティカルポジションにより規定されるスクランブルパラメータを生成し、ビデオデータデスクランブル処理部は、前記スクランブルパラメータを用いてデスクランブル処理することを特徴とするデスクランブル装置。

【請求項13】 トラnsポートパケット単位でスクランブル処理するスクランブル手段とビデオデータ中のビデオシーケンスの先頭を検出するシーケンス先頭検出手段を具備し、シーケンス先頭検出手段により見いだされたビデオシーケンスの先頭を含むパケットにおいてスクランブル手段がスクランブル鍵を更新することを特徴とするスクランブル装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、デジタル符号化された信号の伝送あるいは保管に際し、信号を撹拌し、復号手順を許可されたものだけに与えることによって、再生できる者を限定するためのものであり、主に有料放送などにおける番組へのアクセス制御あるいはVTRやディスク等の蓄積メディアにおける著作権保護のための不正な複製防止などに用いられるスクランブル制御に関するもので特に送信データがMPEG標準（ISO 1175-1, 2, 3 (MPEG1)およびISO 13818-1, 2, 3 (MPEG2)）の1部の規格に準拠したデータに対するものに関する。

【0002】

【従来の技術】 MPEG標準に準拠したデータについてのスクランブル制御については、ISO13818-1のMPEG2のシステムレイヤ規格における記述がある。図11は、MPEG標準のトラnsポートストリームの構成の説明図である。トラnsポートストリームは、188バイトの固定長のパケットで構成されたビットストリームであり、ビデオデータやオーディオデータあるいはその他のデータおよびこれらデータを逆多重化するためのデータ（図では簡単のため省略）およびコンディショナルアクセス情報等のデータをそれぞれ固定長のパケットに変換して多重したデータである。

【0003】 ビットストリーム中のビデオデータについて説明するとビデオデータを構成する読み取りの為の同期ビットをもった最小単位がスライスであり、数個のスライスをもってピクチャを構成する。さらに、複数のピクチャでグループオブピクチャを構成し、1つ以上のグループオブピクチャでビデオシーケンスを構成する。各データの単位には、図では省略しているが同期ビットとヘッダ情報が存在する。ビデオシーケンスは、再生できるデータをすべてを含んだデータ単位であり、ビデオシーケンスの最初のデータから読み取ることで再生可能となる。以上のように構成されたビデオデータを先頭から

分割してトラnsポートパケットを形成するビデオをパケット化する。

【0004】 オーディオやコンディショナルアクセス情報等と同じく188バイトの固定長パケット化されて多重され、トラnsポートストリームが形成される。なお、トラnsポートストリームの規定では、複数のビデオやオーディオの信号も多重できるがここではそれぞれ1つずつの場合を説明した。

【0005】 以上のようにトラnsポートストリームにおいて従来のスクランブル制御方法を説明する。スクランブル鍵の更新タイミングとしては、各パケットの先頭部にあるスクランブルコントロールコード2ビットを用いて行うことが可能である。図12は、従来のスクランブル制御方法による鍵の更新タイミングの説明図である。スクランブルコントロールコードのパターンとして“10”と“11”をもつパケットを作りスクランブルされるパケットを示す。

【0006】 同じパターンのパケットが連続する間を同じスクランブル鍵を用いていることを示し、鍵の更新タイミングでパターンを反転させることでスクランブル鍵更新タイミングを示す。すなわち、コンディショナルアクセス情報パケット中でスクランブル鍵が伝送されてきて、その鍵は、次にスクランブルコントロールコードが反転するタイミングで有効鍵となる。また、スクランブルコントロールフラグのパターンが“00”のパケットはスクランブルしていないパケットである。

【0007】

【発明が解決しようとする課題】 しかしながら前記のような方法では、パケット単位でスクランブルの再生同期を管理することになるので、スクランブル鍵の検出してパケットのデータを再生可能になってもパケット中のデータ自体の再生の同期がとれる位置と必ずしも一致しないため、実際に再生可能になる時間までに遅延が生ずる問題点があった。

【0008】 また、スクランブル処理自体がトラnsポートパケット単位の制御では、十分行えないような処理、例えばスクランブル効果制御を行いビデオデータレベルでの処理が必要な場合（例えば、特願平4-259540号等のスクランブル装置がある。）、単なるパケットヘッダー上のフラグだけでは、スクランブル鍵の更新の同期がとれない問題があった。

【0009】 以上お点に鑑み本発明では、スクランブル処理によって、再生に遅延が生じることなく、また、ビデオデータに対してパケット単位ではないスクランブル処理を行った場合でもスクランブルの鍵更新の管理がパケット単位のスクランブル処理に対する処理と同様に行えるスクランブル制御方法およびそれを実現するスクランブル装置デスクランブル装置を提供することを目的とする。

【0010】

【課題を解決するための手段】本発明の第1の発明は、MPEG標準に準拠したデジタル信号をトランスポートパケット単位で送信し、各データにスクランブルを施してなるスクランブル制御方法において、MPEG標準に準拠したビデオデータ中のビデオシーケンスの先頭をスクランブル鍵の更新タイミングとして用いる方法である。

【0011】本発明の第2の発明は、ビデオデータをトランスポートパケット単位でスクランブル処理するスクランブル制御方法において、ビデオデータのビデオシーケンスの先頭を含むパケットを鍵更新タイミングとする方法である。

【0012】本発明の第3の発明は、少なくとも1ピクチャーより長い更新周期で伝送されるスクランブル鍵とピクチャテンポラルリファレンスより決定されるパラメータをスクランブルを行うパラメータとしてピクチャの先頭において前記パラメータを更新する方法である。

【0013】本発明の第4の発明は、少なくとも1スライスより長い更新周期で伝送されるスクランブル鍵とピクチャテンポラルリファレンスおよびスライスパーティカルポジションより決定されるパラメータをスクランブルを行うパラメータとしてスライスの先頭において前記パラメータを更新する方法である。

【0014】本発明の第5の発明は、ビデオデータにスクランブル処理するビデオスクランブル手段とトランスポートパケット単位でスクランブル処理を施すトランスポートスクランブル手段と前記ビデオスクランブル手段とトランスポートスクランブル手段にスクランブル鍵を更新させるスクランブル鍵更新手段からなり、スクランブル鍵更新手段は、ビデオスクランブル処理手段にビデオデータのビデオシーケンスの先頭毎にスクランブル鍵を更新させ、前記更新されるスクランブル鍵は、前記ビデオシーケンスにおいてスクランブルされたビデオデータ中のビデオシーケンスコードを含むパケット以前に伝送されたパケットで最も最近スクランブルされたパケットのスクランブル処理に用いられた鍵と等しい鍵である構成である。

【0015】本発明の第6の発明は、トランスポートパケット単位でデスクランブル処理するトランスポートデスクランブル手段とスクランブルを施されてなるビデオデータをデスクランブル処理してなるビデオデスクランブル処理と前記二つのデスクランブル手段のスクランブル鍵を更新する鍵更新手段を具備し、ビデオデスクランブル処理部がビデオシーケンスの先頭で鍵を更新し、鍵更新手段は、ビデオデスクランブル手段が鍵を更新する際、その更新鍵を前記ビデオシーケンスの先頭が含まれていたトランスポートパケットの直前でスクランブルされてパケットをデスクランブル処理する鍵と同じ鍵とする構成である。

【0016】本発明の第7の発明は、MPEG標準に準

拠したビデオデータをスクランブル処理するビデオデータ攪拌処理手段とスクランブルパラメータ生成手段とピクチャテンポラルリファレンス検出手段を具備し、ピクチャの先頭において、スクランブル鍵およびテンポラルリファレンスにより規定されるスクランブルパラメータを生成し、ビデオデータ攪拌処理部は、前記スクランブルパラメータを用いてスクランブル処理する構成である。

【0017】本発明の第8の発明は、スクランブルが施されてなるMPEG標準に準拠したビデオデータをデスクランブル処理するビデオデータデスクランブル処理手段とスクランブルパラメータ生成手段とピクチャテンポラルリファレンス検出手段を具備し、ピクチャの先頭において、スクランブル鍵およびテンポラルリファレンスにより規定されるスクランブルパラメータを生成し、ビデオデータデスクランブル処理部は、前記スクランブルパラメータを用いてデスクランブル処理する。

【0018】本発明の第9の発明は、MPEG標準に準拠したビデオデータをスクランブル処理するビデオデータ攪拌処理手段とスクランブルパラメータ生成手段とピクチャテンポラルリファレンス検出手段とスライスパーティカルポジション検出手段を具備し、スライスの先頭において、スクランブル鍵およびスライスが属しているピクチャのテンポラルリファレンスおよびスライスパーティカルポジションにより規定されるスクランブルパラメータを生成し、ビデオデータ攪拌処理部は、前記スクランブルパラメータを用いてスクランブル処理することを特徴とするスクランブル装置。

【0019】本発明の第10の発明は、スクランブルが施されてなるMPEG標準に準拠したビデオデータをデスクランブル処理するビデオデータデスクランブル処理手段とスクランブルパラメータ生成手段とピクチャテンポラルリファレンス検出手段とスライスパーティカルポジション検出手段を具備し、スライスの先頭において、スクランブル鍵およびスライスが属しているピクチャのテンポラルリファレンスおよびスライスパーティカルポジションにより規定されるスクランブルパラメータを生成し、ビデオデータデスクランブル処理部は、前記スクランブルパラメータを用いてデスクランブル処理する構成である。

【0020】本発明の第11の発明は、トランスポートパケット単位でスクランブル処理するスクランブル手段とビデオデータ中のビデオシーケンスの先頭を検出するシーケンス先頭検出手段を具備し、シーケンス先頭検出手段により見いだされたビデオシーケンスの先頭を含むパケットにおいてスクランブル手段がスクランブル鍵を更新する構成である。

【0021】

【作用】本発明のスクランブル制御方法によれば、スクランブル鍵の更新タイミングが単独で再生可能であるビ

デオのデータの単位であるビデオシーケンスの先頭であるのでスクランブル鍵が受信側で与えられデータの再生が可能になった時点よりビデオデータも再生が可能となり遅延が生じずスクランブルを解除できる。また、ビデオデータ以外のデータがトランスポートパケット単位でスクランブル処理されている場合、ビデオシーケンスの先頭のタイミングでトランスポートレベルのスクランブルで使用されているスクランブル鍵に更新してやれば、トランスポートレベルのスクランブルによる再生制御でスクランブル鍵の一元管理が行える。

【0022】また、第2の発明によれば、ビデオシーケンスヘッダを含むパケットをスクランブル鍵の更新タイミングとして用いることで、トランスポートパケットレベルのスクランブル処理の管理だけでもビデオの再生遅延を起こさないスクランブル制御が行える。

【0023】また、第3および第4の発明によれば、スクランブル鍵があれば再生途中でデータ誤り等でスクランブルの再生が一次的に不能になってもビデオデータ中の次のピクチャあるいはスライスの単位でスクランブルの更新周期に比べ短い期間でスクランブルの再生を復帰できる。

【0024】また、第5および第6の発明によれば、第1の発明のスクランブル制御方法によるスクランブル装置およびデスクランブル装置が構成できる。

【0025】また、第7および第8の発明によれば、第3の発明のスクランブル制御方法によるスクランブル装置およびデスクランブル装置が構成できる。

【0026】また、第9および第10の発明によれば、第4の発明のスクランブル制御方法によるスクランブル装置およびデスクランブル装置が構成できる。

【0027】また、第11の発明によれば、第2の発明のスクランブル制御方法によるスクランブル装置が構成できる。

【0028】

【実施例】図1は本発明の第1の実施例におけるスクランブル制御方法の説明図である。以下、本実施例のスクランブル制御方法におけるスクランブル鍵の更新タイミングを説明する。トランスポートストリームには、1つのビデオデータとオーディオデータおよびこれらのコンディショナルアクセスコントロール情報と図中では、省略しているが逆多重化するための情報が含まれている。スクランブル鍵は、コンディショナルアクセス情報パケット（以下CAパケット）中で送られる。

【0029】また、スクランブル処理は、オーディオデータに対してはトランスポートのパケット単位でスクランブル処理が行われ（以下TSスクランブル）、ビデオデータについては、ビデオのビットストリームに依存したスクランブル処理を行う（以下ビデオスクランブル）。TSスクランブルの制御は、従来例と同様に行う。すなわち、スクランブルの対象となるパケットにス

クランブルコントロールコードのパターンを“11”と“10”としてスクランブル処理する。

【0030】その際、スクランブル鍵はCAパケット中で与え、その鍵は、次のスクランブルコントロールコードの反転したパケットから有効になる。次にビデオスクランブルについて説明する。ビデオスクランブルする場合は、トランスポートパケット中のスクランブルコントロールコードは、“00”とする。また、スクランブル鍵の更新タイミングは、ビデオシーケンスの先頭であり、そのときTSスクランブルの有効鍵をビデオスクランブルの有効鍵とする。すなわち、CAパケット中のスクランブル鍵は、次のスクランブルコントロールコードの反転したパケットの出現によって有効となり、さらに、ビデオデータ中のビデオシーケンスの先頭でビデオスクランブルの鍵として有効になる。

【0031】以上のように、本発明の第1の実施例におけるスクランブル制御方法によれば、ビデオデータ中のビデオシーケンスの先頭を新たに鍵更新タイミングとして設けることでトランスポート単位でのスクランブル処理とビデオデータレベルでのスクランブル処理のスクランブル鍵を一元管理できるとともに、ビデオシーケンスが、ビデオデータが再生できる単位になっていることから、デスクランブルを行う際に、スクランブル鍵を取得してから再生が可能になるまでに要する時間を短くすることができ。

【0032】図2は、第2の実施例におけるスクランブル装置の構成図である。前記スクランブル装置は、第1の実施例のスクランブル制御方法に基づくスクランブル信号を生成するものである。図2において、1は、データを所望のアクセス制御を行うための信号を出力し、各処理部を制御するコンディショナルアクセス処理部、2はビデオスクランブル処理部、3は、データを多重化処理する多重化処理部、4は、TSスクランブルを行うTSスクランブル処理部である。

【0033】以上のような構成において以下その動作を説明する。コンディショナルアクセス処理部1は、ビデオスクランブル処理部2およびTSスクランブル処理部4へスクランブル鍵Ksを送るとともに、Ksを含んだCAデータを多重化処理部3へ送る。CAデータは、スクランブル鍵Ksとどのデータにスクランブル処理を行うかを示す信号が含まれる。ビデオデータは、ビデオスクランブル処理部2でコンディショナルアクセス処理部1からのスクランブル鍵Ksでスクランブル処理され多重化処理部3へ送られる。

【0034】この際、ビデオスクランブル処理部2は、ビデオシーケンスの先頭を検出し、コンディショナルアクセス処理部1へ検出信号を送る。コンディショナルアクセス処理部1では、現在TSスクランブルで有効にしているスクランブル鍵を送る。ビデオスクランブル処理部2では、受け取り後直ちに有効鍵としてスクランブル

処理する。多重化処理部3は、CAデータで示されているデータのバケットのスクランブルコントロールコードに“11”あるいは“10”をつけてバケット化し多重するとともに、CAデータからCAバケットデータを生成しバケット化して多重する。図3は、多重化処理部の構成図である。

【0035】図3において、5は、ビデオデータ中のシーケンスヘッダを検出するシーケンスヘッダ検出部、6は、バケット生成多重化部である。多重化されるデータバケット生成多重化部6に入力される。この際ビデオデータは、シーケンスヘッダ検出部5への入力される。シーケンスヘッダ検出部5では、ビデオシーケンスの先頭を検出し、検出信号をバケット生成多重化部6へ送る。バケット生成多重化部6では、CAデータに従ってスクランブルコントロールコードを各バケットにつける。ただし、ビデオスクランブル処理のみを行うビデオバケットのスクランブルコントロールコードは“00”とする。

【0036】この際、シーケンスヘッダ検出部5からの検出信号を受けビデオシーケンスの先頭を含んだバケットを多重化した後毎にスクランブルコントロールコードを“11”から“10”あるいは“10”から“11”につけるコードを反転するとともに、次の検出信号を受け取るまでスクランブルの対象となるバケットには、同じパターンをつける。さらに、検出信号を受け取り後、直ちにCAリクエスト信号を送り、新たなCAデータを受け取る。受け取ったCAデータは、TSスクランブルを行ったバケットのPIDおよびビデオスクランブルを行ったかを示す信号をCAデータより変換してバケット化し多重化し、多重化したCAデータは、次のシーケンスの先頭検出後のスクランブルコントロールコードをつける作業に用いる。

【0037】TSスクランブル処理部4では、スクランブルコントロールコードが“10”あるいは“11”となっているバケットのヘッダ部を除いたペイロードにスクランブルを行う。この際用いるスクランブル鍵Ksは、コンディショナルアクセス処理部1が多重化処理部3へCAデータを送った際のCAデータに含まれるKsと同じものをコンディショナルアクセス処理部1が多重化処理部3にCAデータを伝送した直後にTSスクランブル処理部4に送る。受け取ったKsは、スクランブルコントロールコードが反転したバケットから有効鍵となり、スクランブル処理に用いられる。スクランブル処理とりては、ブロック暗号でもよいし、乱数加算を行うものでもよく公知の技術で実現できる。

【0038】以上のように本実施例のスクランブル装置によれば、実施例1のスクランブル制御方法にしたがった鍵更新をおこなったスクランブルデータを生成でき、ビデオレベルのスクランブルとTSレベルのスクランブルを同時に行える。

【0039】図4は、本発明の第3の実施例におけるデスクランブル装置である。これは、第2の実施例により

生成されたスクランブルデータをデスクランブル処理するものである。図4において、7は、コンディショナルアクセス処理部、8は、TSデスクランブル処理部、9は、逆多重化処理部、10は、ビデオデスクランブル処理/ビデオ再生処理部、11は、オーディオ再生処理部である。

【0040】以上のように構成されたこの実施例のデスクランブル装置において、以下その動作を説明する。コンディショナルアクセス処理部7は、逆多重化処理部9よりCAデータをうけるとTSデスクランブル処理部8へ直ちに送信する。逆多重化処理部9は、多重化されてきたデータをビデオデータオーディオデータにそれぞれ逆多重化する。その際、ヘッダ中のスクランブルコントロールフラグが“10”または“11”のバケットについては、そのバケット全体をTSデスクランブル処理部8伝送し、デスクランブル処理されたバケットを受け取り逆多重化処理する。

【0041】TSデスクランブル処理部8では、コンディショナルアクセス処理部7から送られてきたスクランブル鍵Ksで逆多重化処理部9から送られてくるバケット中のペイロードをデスクランブル処理するとともに、スクランブルコントロールコードを“00”に変更し、逆多重化処理部9へ返送する。この際、コンディショナルアクセス処理部7から送られてくるKsは一次記憶され、スクランブルコントロールコードの反転の際に有効鍵となるとともに、TSデスクランブル処理部は、コンディショナルアクセス処理部7に鍵更新されたことを示す更新タイミング信号を送る。

【0042】ビデオスクランブル処理/ビデオ再生処理部10では、ビデオデータ中のビデオシーケンスの先頭を検出する毎にスクランブル鍵要求信号をコンディショナルアクセス処理部7へ送り、TSスクランブル処理で有効になっているスクランブル鍵Ksを受け取り、受け取った鍵を直ちに用いてデスクランブル処理とビデオデータ再生処理を行う。オーディオ再生処理部11は、逆多重化処理部9から送られてくるデスクランブル処理された音声データを再生する。

【0043】以上のように本実施例のデスクランブル装置によれば、第1の実施例のスクランブル制御方法にしたがって生成されたスクランブルデータをデスクランブル処理できる。

【0044】図5は、本発明第4の実施例のスクランブル制御方法の説明図である。本実施例は、第1の実施例のようにビデオスクランブルにおいてビデオシーケンス毎に鍵の更新を行った場合の制御方法を示している。スクランブル鍵Ksは、ビデオシーケンスあたり1つの鍵が有効鍵として与えられる。そして、この有効鍵をもとにピクチャヘッダおよび1スライス期間中以下のスクランブルパラメータを生成してスクランブル処理する。まず、ピクチャヘッダ期間では、有効鍵とピクチャヘッダ



中のテンポラルリファレンス値の64乗を法として加算した結果をスクランブルパラメータとする。また、スライス中では、有効鍵とそのスライスが含まれているピクチャのテンポラルリファレンスおよびスライスパーティカルポジションを2の64乗を法として加算したものを各々スクランブルパラメータとすし、それぞれの値をスクランブル処理する際の乱数発生器の初期値として利用する。

【0045】以上のように本実施例のスクランブル制御方法によれば、1ビデオシーケンスで1回スクランブル鍵でスクランブルパラメータを変換する場合がビデオシーケンス中伝送エラー等で再生の同期がはずれると以後、ビデオシーケンスの最後まで再生ができなくなるのに対して、ピクチャヘッダおよびスライス毎にスクランブルパラメータを更新するのでエラー等で再生ができなくてもスライス単位で再生の同期を復帰させることができる。また、特に、各同期の取れる位置でのスクランブルパラメータは、ピクチャのテンポラルリファレンスおよびスライスパーティカルポジションで簡易に計算できるので、エラーが複数のスライスにわたる場合でも再生同期を復帰させることができる。

【0046】図6は、本発明の第5の実施例のスクランブル装置における構成の説明図である。これは、第4の実施例のスクランブル制御方法によるスクランブル信号を生成するスクランブル装置であり、また、第2の実施例におけるビデオスクランブル処理部2を構成することができるものである。図6において、12は、入力信号中のビデオシーケンスの先頭を検出し、検出信号を出力するシーケンスヘッダ検出部、13は、スライスのヘッダ部を検出し、スライスパーティカルポジションの値を出力するスライス検出部、14は、ピクチャ先頭を検出し、テンポラルリファレンスの値を出力するピクチャヘッダ検出部、15は、入力データ中のスクランブル処理するビットを検出するスクランブル位置検出部、16は、乱数発生器を初期化する値を生成する乱数初期値生成部、17は、乱数発生器、18は排他的論理和回路である。

【0047】以上のように構成された本実施例のスクランブル装置について以下その動作を説明する。入力信号は、MPEG標準に準拠したビデオデータである。スクランブル鍵Ksは、シーケンスヘッダ検出部12が検出信号を出力する毎に乱数初期値生成部に入力される。そして、ピクチャヘッダ検出部14からのテンポラルリファレンス信号をうけると図5のFpの処理にしたがって、スクランブルパラメータを計算し、乱数の初期値として乱数発生器17へ出力する。

【0048】また、スライス検出部13がスライスのパーティカルポジションを送ってきたとき、乱数初期値生成部16は、その直前に送られてきたピクチャのテンポラルリファレンス値と今送られてきたパーティカルポジ

ションをから図5のFsの処理に従ってスクランブルパラメータを計算し、乱数発生器17へ送る。以上の処理で乱数発生器17は初期化される。スクランブル位置検出部15は、入力信号中の"dct\_type"および"DCT係数のDC成分の値を示す信号を検出し、そのタイミングを乱数発生器17へ送る。乱数発生器17は、スクランブル位置検出部15からの信号があるときのみ乱数を出力し、排他的論理和回路18で入力信号に排他的論理和される。

【0049】以上の実施例によれば、実施例4のスクランブル制御方法によるスクランブル信号を生成することができる。

【0050】図7は、本発明の第6の実施例におけるデスクランブル装置の構成図である。これは、第5の実施例のスクランブル装置で生成されたスクランブル信号を再生するものであり、第3の実施例におけるビデオデスクランブル処理/ビデオ再生処理部10の詳細を示した図である。図7において、19は、入力信号中のビデオシーケンスの先頭を検出し、検出信号を出力するシーケンスヘッダ検出部、20は、スライスのヘッダ部を検出し、スライスパーティカルポジションの値を出力するスライス検出部、21は、ピクチャ先頭を検出し、テンポラルリファレンスの値を出力するピクチャヘッダ検出部、22は、入力データ中のスクランブル処理されたビットを検出するスクランブル位置検出部、23は、乱数発生器を初期化する値を生成する乱数初期値生成部、24は、乱数発生器18と同じ乱数発生器、25は排他的論理和回路、26はビデオ再生処理部である。

【0051】以上のように構成された本実施例のスクランブル装置について以下その動作を説明する。スクランブル鍵Ksは、シーケンスヘッダ検出部19が検出信号を出力する毎に乱数初期値生成部23に入力される。そして、ピクチャヘッダ検出部21からのテンポラルリファレンス信号をうけると図5のFpの処理にしたがって、スクランブルパラメータを計算し、乱数の初期値として乱数発生器24へ出力する。また、スライス検出部20がスライスのパーティカルポジションを送ってきたとき、乱数初期値生成部23は、その直前に送られてきたピクチャのテンポラルリファレンス値と今送られてきたパーティカルポジションをから図5のFsの処理に従ってスクランブルパラメータを計算し、乱数発生器24へ送る。

【0052】以上の処理で乱数発生器24は初期化される。スクランブル位置検出部22は、入力信号中の"dct\_type"および"DCT係数のDC成分の値を示す信号を検出し、そのタイミングを乱数発生器24へ送る。乱数発生器24は、スクランブル位置検出部22からの信号があるときのみ乱数を出力し、排他的論理和回路25で入力信号に排他的論理和される。したがって、同じ乱数発生器の出力が同じ位置にもう一度排他的論理和加算さ

れたことになりデスクランブル処理された信号をえる。その信号はビデオ再生処理部26で再生される。

【0053】以上の実施例によれば、実施例4のスクランブル制御方法により生成されたスクランブル信号をデスクランブル処理できる。

【0054】図8は、本発明の第7の実施例におけるスクランブル制御方法の説明図である。同図は、トランスポート単位でスクランブルを行うシステムにおけるスクランブル鍵の更新タイミングを示している。スクランブルコントロールコードによってスクランブルの有無および鍵の更新タイミングを示すのは、従来例と同様である。ただ、スクランブルフラグ反転位置をビデオシーケンスの先頭とする。

【0055】以上の制御方法によれば、スクランブル鍵の取得からビデオの再生までに要する時間を短くできる。図9は、鍵更新による新しい鍵の取得からビデオ再生までに要する時間を説明したものである。鍵更新タイミングが特に規定せず適当に発生させた場合、鍵更新位置から各パケットは、デスクランブル処理されるがデータを最初に受信したときなどのように以前のデータが再生されていない場合、シーケンスヘッダ内の再生に必要なデータ等がなくビデオデータが再生可能になるには最も近いビデオシーケンスの先頭からとなり、図9のTdだけの鍵更新時刻よりも再生が遅れてしまうことになり最大1ビデオシーケンス分の遅れを見積もる必要がある。一方、本実施例のようにビデオシーケンスと鍵更新位置を一致させておくとTdが0になりビデオデータの再生の遅れを解消できる。

【0056】図10は、本発明の第8の実施例のスクランブル装置の構成図である。これは、第7の実施例のスクランブル制御方法にしたがってスクランブル信号を生成するスクランブル装置である。図10において、27はコンディショナルアクセス処理部、28は、シーケンスヘッダ検出部、29は、多重化処理部、30は、TSスクランブル処理部である。

【0057】以上のように構成されたスクランブル装置において以下その動作を説明する。まず、ビデオデータは、MPEG標準に準拠したデータである。コンディショナルアクセス処理部27は、スクランブル処理を行うデータおよびスクランブル鍵を含んだCAデータを多重化処理部29に送る。多重化処理部29では、CAデータをパケット化して多重すると共にCAデータの指示にしたがって、スクランブル処理を指示されたデータを含むパケットのヘッダ中のスクランブルコントロールコードを“1”あるいは“10”とし、スクランブルしないパケットは“0”として多重化処理する。

【0058】この際、シーケンスヘッダ検出部28は、ビデオデータ中のビデオシーケンスの先頭を検出し、多重化処理部29およびコンディショナルアクセス処理部27へ検出信号を送る。多重化処理部29では、検出信

号を受け取ると現在までに送られてきた内の最新のCAデータに基づきスクランブルを行うパケットにつけていたスクランブルコントロール信号を“1”から“10”あるいは“10”から“11”にビット反転させて以後、次の検出信号を受け取るまで一定のパターンをつけ続ける。

【0059】また、検出信号を受けたのちコンディショナルアクセス処理部27から新たなCAデータが送られてくるとそのデータをパケット化し、多重処理するとともにCAデータを保持し、次の検出信号時のスクランブルコントロールコードの制御の際に有効にする。以上の処理を行いながらビデオとオーディオおよびCAデータをパケット化し多重数し、TSスクランブル処理部30へ送る。コンディショナルアクセス処理部27では、シーケンスヘッダ検出部28からの検出信号毎にCAデータを多重化処理部29へ送ると共に、TSスクランブル処理部30からの鍵要求信号を受ける毎に送る。

【0060】したがって、送られるKsは、多重化処理部29に送った同じKsを含むCAデータが有効になっている期間と有効期間が一致するように送られることになる。TSスクランブル処理部30では、スクランブルコントロールコードが反転したパケットを受け取る毎にスクランブル鍵要求信号をコンディショナルアクセス処理部へ送りスクランブル鍵Ksを受け取り、Ksでスクランブルコントロールコードが“10”または“11”になっているパケットをスクランブル処理する。

【0061】以上の実施例のスクランブル装置により、実施例7のスクランブル制御方法にしたがったスクランブル信号を生成するスクランブル装置が実現できる。シーケンスヘッダ検出部28を設けてビデオシーケンスの先頭を含むパケットを容易に検出できると共に、多重化処理部でスクランブルの対象となるパケットに予めスクランブルコントロールフラグをつけることでTSスクランブルの機能は、デスクランブル処理する場合と同様の処理を行うことで実現できる。

【0062】なお、本実施例では、伝送データとして、ビデオデータとオーディオデータを1つずつ含んだビットストリームを考えたが、さらに複数のデータを含むものでもよいし、複数のプログラムを多重化したデータについても同様に考えられる。

【0063】また、本実施例においては、CAデータについての暗号化について触れなかったが、通常これら一部は暗号化して送ることが多く、これらは、従来のデジタルデータの暗号化技術により実現化能である。

【0064】また、第1の実施例において、TSスクランブルについてその鍵更新周期をスクランブルコントロールコードとしたが、それ以外の方法であってもよく、ビデオデータのシーケンスヘッダ時にTSスクランブルで有効な鍵をビデオスクランブルにも使うならばTSスクランブルの鍵更新方法は他の方法でもよい。

【0065】また、第2の実施例において、TSスクラ

ンブル処理を多重化処理の後に行っているが多重化処理の時点で同時にスクランブルする構成も考えられる。また、TSスクランブルの鍵の更新タイミングをビデオデータ中のビデオシーケンスの先頭のタイミングを利用して行ったが、単に一定時刻毎に行うものでもよいし、全く異なる方法を用いてもよい。

【0066】また、第3の実施例において、TSスクランブル処理部は、逆多重化処理部からスクランブルされたデータを受け取りデスクランブル処理してそれを再び逆多重化処理部にcaesす構成であるが、デスクランブル処理部でデスクランブル処理したビットストリームを生成し、逆多重化処理部におくるような直列に接続された構成も考えられる。

【0067】また、第4の実施例において、スクランブルパラメータを生成する関数としてFpとFsを用いたが、他の発生方法を用いてもよい。また、ピクチャヘッダ中にスクランブルの対象となるコードがない場合には、スライス毎にスクランブルパラメータを生成するだけの構成も考えられるし、また、ピクチャ単位での再生同期で十分と考えられる場合には、ピクチャ単位でスクランブルパラメータを生成し、1ピクチャ間これを有効にすることでもよい。

【0068】また、第5の実施例において、スクランブル処理する位置をdct\_typeとDCT係数のDC成分としたが、それ以外のコードを選択することも考えられし、全く異なったスクランブル処理でもよい。また、スクランブルパラメータの用い方も乱数発生器を初期化する以外の方法でも処理を規定するものであればよい。

【0069】また、第6の実施例においては、デスクランブル処理とビデオ再生処理を直列に配置しているが、ビットストリーム中の特定のコードを検出する処理などは、ビデオ再生処理部にも必要な処理であり、これらの部分を共通化することによる一体化した構成も考えられる。

【0070】また、第7の実施例においてスクランブル鍵更新タイミングをスクランブルコントロールコードを用いて行っているが、鍵の更新タイミングをビデオシーケンスを含むパケットに一致させるのであれば別の方法でもよい。また、第8の実施例以外の構成でも実施例8のスクランブル制御方法を実現するのであれば別の構成も考えられる。

【0071】

【発明の効果】以上説明したように、本発明によれば、MPEGのトランスポートストリーム中のデータのスクランブル制御を行う際に、スクランブル鍵の更新タイミングとしてビデオシーケンスの先頭の位置を用いること

でビデオデータの再生に必要な時間を短縮でき、また、ビデオ特有のスクランブル処理をする場合でもトランスポートパケット単位でのスクランブル処理と鍵の管理を一元化でき、その実用的効果は大きい。

【図面の簡単な説明】

【図1】本発明の第1の実施例におけるスクランブル制御方法の説明図

【図2】本発明の第2の実施例におけるスクランブル装置の構成図

【図3】同実施例の多重化処理部の構成図

【図4】本発明の第3の実施例におけるデスクランブル装置の構成図

【図5】本発明の第4の実施例におけるスクランブル制御方法の説明図

【図6】本発明の第5の実施例におけるスクランブル装置の構成図

【図7】本発明の第6の実施例におけるデスクランブル装置の構成図

【図8】本発明の第7の実施例におけるスクランブル制御方法の説明図

【図9】本発明の第7の実施例における鍵更新による新しい鍵の取得からビデオ再生再生に要する時間の説明図

【図10】本発明の第8の実施例におけるスクランブル装置の構成図

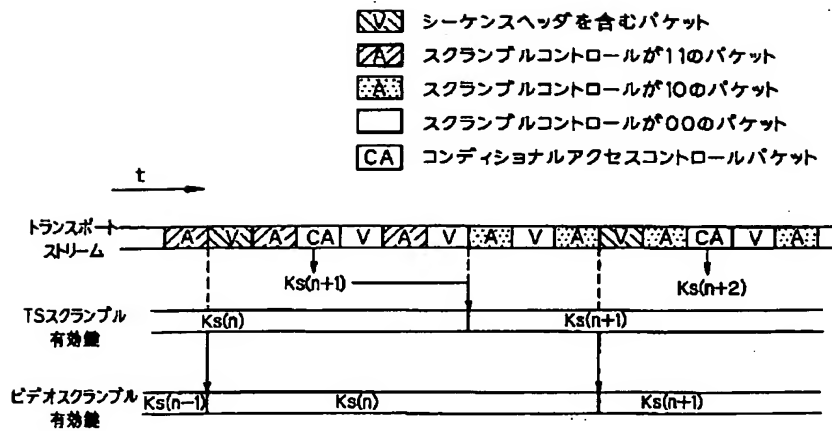
【図11】MPEG標準のトランスポートストリームの構成の説明図

【図12】従来のスクランブル制御方法の説明図

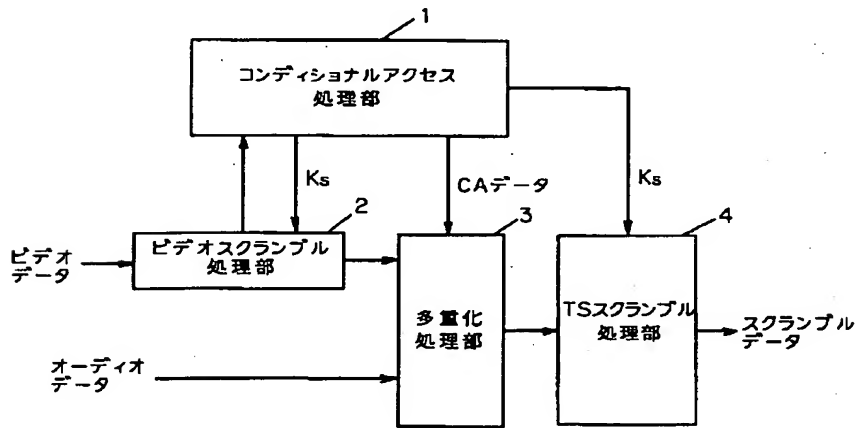
【符号の説明】

- 1、7、27 コンディショナルアクセス処理部
- 2 ビデオスクランブル処理部
- 3、29 多重化処理部
- 4、30 TSスクランブル処理部
- 5、12、19、28 シーケンスヘッダ検出部
- 6 パケット生成多重化部
- 8 TSデスクランブル処理部
- 9 逆多重化処理部
- 10 ビデオデスクランブル処理/ビデオ再生処理部
- 11 オーディオ再生処理部
- 13、20 スライス検出部
- 14、21 ピクチャヘッダ検出部
- 15、22 スクランブル位置検出部
- 16、23 乱数初期値生成部
- 17、24 乱数発生器
- 18、25 排他的論理和回路
- 26 ビデオ再生処理部

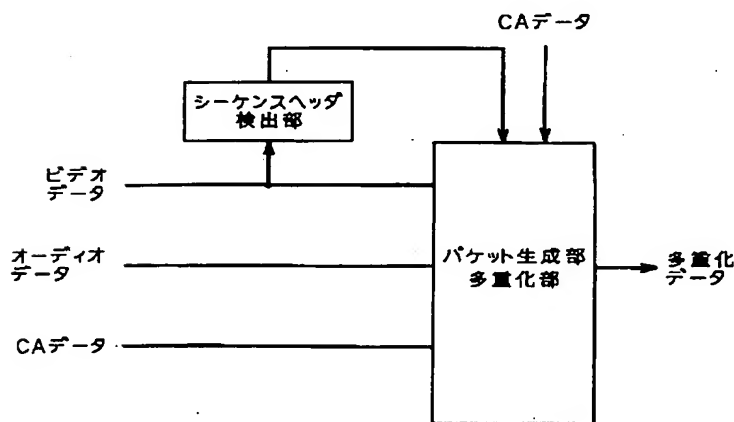
【図1】



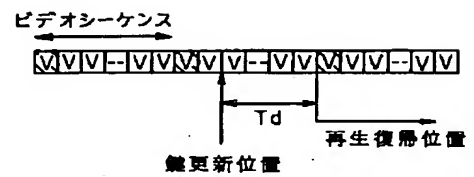
【図2】



【図3】

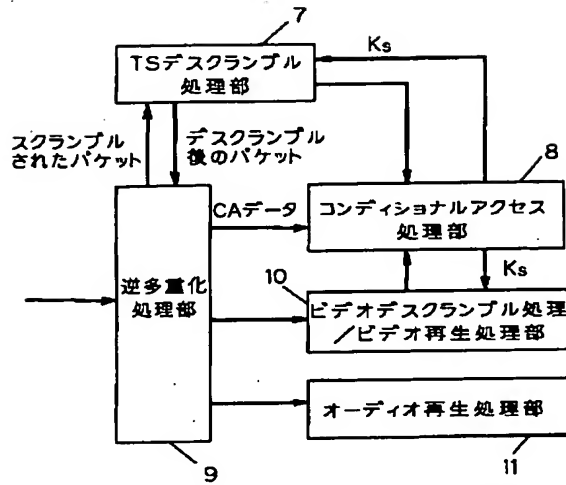


【図9】



Best Available Copy

【図4】

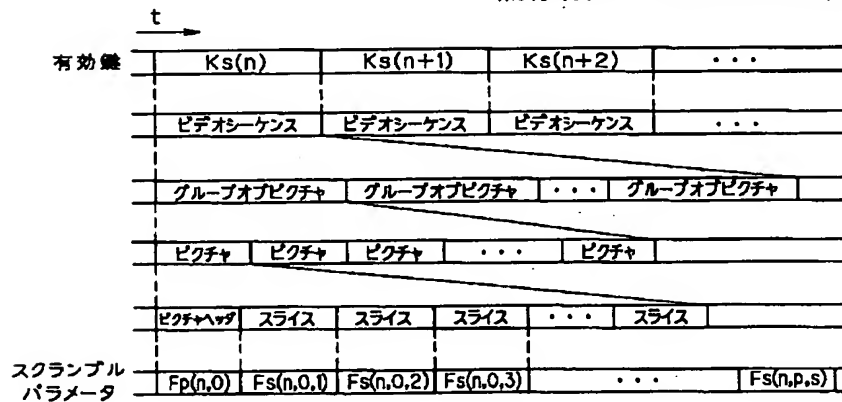


【図5】

$$Fp(n,p) = Ks(n) + p \mod 2^{64}$$

$$Fs(n,p,s) = Ks(n) + p + s \mod 2^{64}$$

p: ピクチャのテンポラルリファレンスの値  
n: スライスパーティカルポジションの値



【図6】

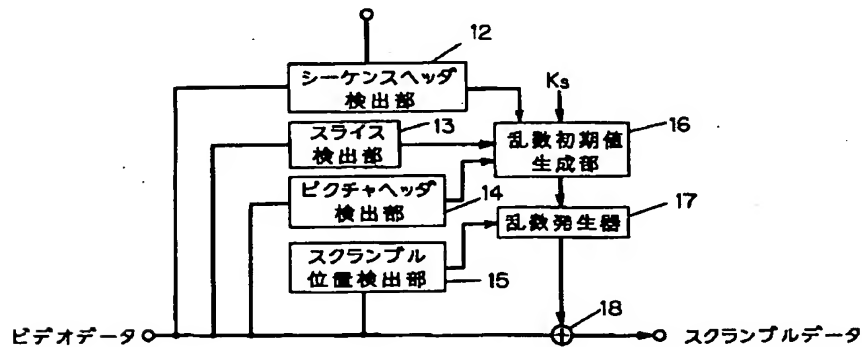


Figure 1 is a block diagram of a video reproduction system. It includes the following components and connections:

- 19**: シーケンスヘッダ検出部 (Sequence Header Detection Unit)
- 20**: スライス検出部 (Slice Detection Unit)
- 21**: ピクチャヘッダ検出部 (Picture Header Detection Unit)
- 22**: スクランブル位置検出部 (Scrambling Position Detection Unit)
- 23**: 乱数初期値生成部 (Random Initial Value Generation Unit)
- 24**: 乱数発生器 (Random Number Generator)
- 25**: A circular adder symbol ( $\oplus$ )
- 26**: ビデオ再生処理部 (Video Reproduction Processing Unit)

The signal flow is as follows:

- Input 19 is connected to block 19.
- Block 19 outputs to block 20.
- Block 20 outputs to block 23.
- Block 21 outputs to block 23.
- Block 22 outputs to block 24.
- Block 23 outputs to block 24.
- Block 24 outputs to block 25.
- Block 25 outputs to block 26.
- There is a feedback loop from the output of block 25 back to the input of block 19.
- Block 26 is labeled "ビデオ再生処理部" (Video Reproduction Processing Unit).

[Box with diagonal line] スランブルフラグが01の packets  
 [Box with dotted pattern] スランブルフラグが10の packets  
 [Box with A] オーディオ packets  
 [Box with V] ビデオ packets  
 [Box with CA] コンディショナルアクセス情報 packets

ビデオシーケンス

V V V -- V V V V V V -- V V V V V V -- V V V V -- V V V

t

V A V V V CA -- A V V V V A V A CA -- A V V A V CA A V V A V V

11 10 11 10

スクランブル コントロール

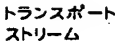
$Kp(n+1)$   $Kp(n+2)$   $Kp(n+3)$

有効鍵  $K(n-1)$   $K(n)$   $K(n+1)$   $K(n+2)$

Figure 1 is a block diagram of a scrambling system. It consists of the following components and data flows:

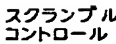
- ビデオデータ** (Video Data) and **オーディオデータ** (Audio Data) are input to the **多重化処理部** (Multiplexing Processing Unit).
- The **多重化処理部** outputs **CAデータ** (CA Data) to the **シーケンスヘッダ検出部** (Sequence Header Detection Unit) and the **コンディショナルアクセス処理部** (Conditional Access Processing Unit).
- The **シーケンスヘッダ検出部** outputs **シーケンスヘッダ** (Sequence Header) to the **コンディショナルアクセス処理部**.
- The **コンディショナルアクセス処理部** outputs **Ks** to the **TSスクランブル処理部** (TS Scrambling Processing Unit).
- The **多重化処理部** outputs data to the **TSスクランブル処理部**.
- The **TSスクランブル処理部** outputs **スクランブルデータ** (Scrambled Data).

\_\_\_\_\_



【例 12】

- 



Best Available Copy

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKewed/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**